Breckland Council

INFORMATION SECURITY POLICY

Information security policy and guidelines

Version Control

	Last Modified	Last Modified By	Document Changes
0.1	02/06/2023	Ben Meen	First draft
0.2	14/06/2023	Ben Meen	Grammatical changes and update to 5.8.2
1.0	22/06/2023	Ben Meen	Incorporation of CMT/JIE

Contents

1 Table of Contents

1. Introduction

1.1 Purpose

The purpose of this document is to set out the Information Security Policy that applies to Breckland Council, to protect the confidentiality, integrity, and availability of data and the ICT systems that the Council depends on to deliver its mission, and to support day-to-day business activities.

All staff and members have a duty and responsibility both to the Council and the people of Breckland to protect these ICT assets from unauthorised use, disclosure, access, modification and destruction. This policy supports compliance with a number of legislative policies and legal requirements, as articulated in section 3 - Compliance with Legislation and other standards.

1.2 Governance framework

The governance arrangements relating to this policy follow a 7-step approach

Step No.	By	Activity
1	Breckland ICT	Defines its policies and standards
2	Breckland ICT	Agree and document the processes to be followed and (where appropriate) their quality
3	Breckland ICT	Implements the necessary processes to deliver the services to that quality
4	Breckland ICT	Monitors adherence to the processes
5	Breckland ICT	Reports breaches and general performance
6	Breckland Management	Enforces policies and procedures through the designated governance groups e.g. CMT
7	Breckland ICT	Reviews these arrangements annually

1.3 Scope

1.3.1 Who the Policy applies to

The Breckland Information Security Policy applies to:

- All staff
- All elected Members of the Council
- All employees and agents of other organisations who directly or indirectly support or use the Council's computer systems or networks e.g., Capita
- All temporary and agency staff directly or indirectly employed by the Council

1.3.2 Where the Policy applies

The policy remains in force regardless of location and specifically includes those who work at Council offices, at home (including Members), in the field, or any other location where the user is using the Council's ICT services.

1.3.3 What the Policy applies to

The Information Security Policy covers any data, device, software, or other assets of the environment that supports information-related activities, including:

- All Council Information
- All physical data and voice communications networks and components
- All software applications resident on applications servers, file servers and networking equipment
- All ICT systems and accompanying software applications
- All storage media including paper
- Internet and email services

1.4 Principles

The information the Council manages is a fundamental asset and is protected against the adverse effects of failures in confidentiality, integrity, availability and compliance with legal requirements, which may otherwise occur.

Achieving this objective is dependent on all staff, elected Members, and employees of supporting organisations who use the Council's ICT systems, complying with this policy, and alignment to the following principles:

- Information will be protected in line with all relevant Council policies and legislation
- Information will be available solely to those who have a legitimate need for access
- Information will be classified according to the Council's data classification guidelines
- The integrity of information will be maintained
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification
- Information will be protected against unauthorised access

1.5 Information security objectives

- To ensure the confidentiality, integrity and availability of Council-managed information, including all personal data as defined by the GDPR based on good risk management, legal regulatory and contractual obligations, and business need
- To provide the resources required to develop, implement, and continually improve the information security practices
- To effectively manage third party suppliers who process, store, or transmit information to reduce and manage information security risks
- To implement a culture of information security and data protection through effective training and awareness

2. Roles and responsibilities

Role	Responsibilities
All Staff and Members	• Read, fully understand, and comply with their obligations with respect to this ICT Security Policy • Remain up to date with any mandatory IT training • Report any suspected or actual breaches of this policy to the ICT helpdesk (by phone 01362 656277 or email: helpmeit@breckland.gov.uk)
Service Managers	• Enforce all ICT security procedures and ensure that all aspects of this security policy are adhered to within their service area • Take appropriate steps to ensure that their staff comply with the policy • Ensure staff are up to date with any mandatory IT training • Identify any sensitive information that is used within their service and ensure that robust security arrangements are in place for securing ICT (e.g. health or financial records, information about vulnerable people)
The ICT Manager	• Ensure the integrity of the Council's ICT services • Obtain approval from CMT, Members, etc. for the security policy • Enforce the policy and coordinate the Council's response to any breaches in cooperation with the DPO

Breckland ICT	• Produce this policy and annually review its provisions • Monitor compliance with the policy • Communicate its contents to users and provide appropriate guidance • Implement the technical and procedural provisions of this ICT Security Policy • Maintain written procedures and ensure that their staff are appropriately trained and equipped to implement them • Monitor ICT systems through a combination of automatic and manual checks to ensure compliance with this policy • Log and investigate actual or suspected breaches of this policy and report the findings to the ICT Manager for action
HR	• Obtain signoff of this policy by all staff and Members and ensure the policy aligns with the Council's employment and disciplinary arrangements
Audit	• Audit and make recommendations for improving the Council's security arrangements

3. Compliance with Legislation and other standards

3.1 Legislation

This policy is designed to ensure that the Council complies with key legislation in this area including the following;

Legislation	Description
Data Protection Act 2018 and UK GDPR	https://www.legislation.gov.uk/ukpga/2018/12/contents The UK's current Data Protection Act came into force on 25th May 2018, alongside the General Data Protection Regulation (GDPR). The Act gives individuals rights over their personal data and protects them from the erroneous use of their personal data. The Act also imposes responsibilities and requirements on any organisation that handles personal data, obligating them to comply with a number of important principles and legal obligations.
Freedom of Information Act 2000	Ensures public access to organisational records and information in the public/government domain
Privacy and Electronic Communications Regulations 2003	The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.
Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011	An amendment to the Privacy and Electronic Communications Regulations in 2011 obliged websites to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies.
The Regulation of Investigatory Powers Act 2000 (RIPA)	Monitoring (but not recording) communications is authorised for the purpose of determining whether they are personal or business communications The interceptor must make all reasonable efforts to inform every person who may use the telecommunication system in question that communications…. may be intercepted

Computer Misuse Act 1990	This makes it an offence for a person to knowingly attempt to access data or systems without proper authorisation
Human Rights Act 1998	Everyone has the right to respect for his private and family life, his home and his correspondence and there shall be no interference by a public authority with the exercise of the right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others
The Defamation Act 2013	The author of a libellous message is responsible for it and liable for any damage it causes to the reputation of another. The author's employer may also be liable.

3.2 Standards and best practice

ISO27001 is a code of practice supported by industry and the Government. The objective of this policy is to ensure compliance with (but not certification to) those aspects of ISO27001 which are appropriate for the Council.

3.3 Connectivity – Public Sector Network (PSN)

The PSN is the government's high-performance secure network, which helps public sector organisations work together, reduce duplication and share resources. Breckland Council aims to achieve annual compliance with the PSN certification programme. Adherence to the Information Security Policy assists Breckland in achieving this aim.

4. Monitoring and enforcement

4.1 General

The Council's ICT Systems are designed to help employees and members in the performance of their work. Negligent, improper or unlawful use of the Council's Communication Systems may create legal obligations for or lead to criminal prosecution against any employee or the Council. The Council will not tolerate abuse, unauthorised or unsecured use of its ICT Systems.

Breach of any term of this Policy may lead to disciplinary action or to termination of any engagement of a supplier of any ICT goods / service. It may also result in civil or criminal action being taken against any employee and / or the Council. An example of a breach may result from the use of the Council's ICT systems to access websites with unsuitable contents such as child pornography, etc. See below for examples of major and minor Breaches.

The Council reserves the right to monitor internet & email usage by staff and members. Checks on devices may also be carried out to ensure that unlicensed or trial software is not installed on the Council's ICT equipment.

Monitoring of a specific user will only be carried out with authorisation from the HR Manager or relevant Assistant Director in the case of staff, or from the Chief Executive in the case of members.

4.2 Examples of breaches

Breach	Category
Copying or sharing with others software, music or movies without the written permission of the copyright owner.	Major
Hacking into, meddling with, or damaging any other computer or service. e.g. trying to "break into" or "crash" another computer on the Internet.	Major

Possessing, accessing or using any unauthorised hacker tools, whether hardware or software based. e.g. “packet sniffers” and “password crackers”.	Major
Viewing, downloading, storing, sending, or giving access to material deemed as objectionable by the Censorship Act 1996 (WA). eg. materials such as child pornography, incitement to violence, torture, and bestiality.	Major
Harassing any person e.g. sending obscene messages, language, pictures or other materials; issuing threats of bodily harm; contacting a person repeatedly without legitimate reason; disrupting another person's lawful pursuits; and invading another person's privacy.	Major
Unauthorised use of access accounts and/or passwords: Deliberately Inadvertently	 Major Minor

Please note that breaches are not necessarily limited to those outlined above.

4.3 Dealing with breaches

Breaches of security must be reported to the ICT Service desk (helpmeit@breckland.gov.uk or 01362 656277) as soon as possible. The ICT service desk will record any breaches by means of a formal logging and follow-up system. For each incident this will include the investigation of the problem cause,

options for the prevention of recurrence, maintenance of an audit trail, informing those affected; ensuring recovery is achieved with minimal delay and the management of a review process. The audit trail will be suitable for internal statistical analysis and for use as evidence on contractual and legal issues such as computer misuse and data protection or investigation by PSN / National Cyber Security Centre (NCSC), if required.

The responsibility for the recovery from an incident or failure will be restricted to staff with specific support responsibilities within Breckland ICT.

Where a breach is discovered Breckland ICT and the DPO will undertake the appropriate enforcement action. For minor or inadvertent breaches this may include:

- Technical changes to physically prevent further such breaches
- Informal warnings regarding future behaviour
- Informal warning to the Service Manager
- For major or persistent breaches by staff the Council's disciplinary procedure will be invoked.
- For major or persistent breaches by Members the Council's Constitution and Members' Code of Conduct will apply.

If the Council is affected by an incident which involves (or is likely to involve) a breach of personal data, then under some circumstances there will be an obligation under the GDPR to notify the ICO.

5. Security policies and measures

5.1 General

All ICT systems are for the sole use of the Council. The Council owns all data that exists on these systems and has the right to access, edit and delete it.

All of the Council's servers, WAN and associated LAN data and voice communications equipment are managed by Breckland ICT. Data networks are managed in such a way as to prevent unauthorised logical and physical connection, and to detect unauthorised connection should this occur. Data communications protocol filtering mechanisms are also employed to restrict network access to authorised users.

No unlicensed or unauthorised software is permitted on any of the Council's ICT systems. Trial or evaluation software should not be installed on the Council devices without the explicit consent of Breckland ICT in writing.

Executable files (such as those of format .exe or .msi) must not be installed on Council equipment except by Breckland ICT or by their written direction.

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is prohibited.

Breckland ICT operates formal change control procedures prior to implementing any request to install / upgrade / change any application software. For this reason you must contact the Breckland ICT helpdesk on 01362 656277 or helpmeit@breckland.gov.uk well in advance otherwise the request may be rejected or work delayed. ICT sign off must be received prior to procuring any new software or IT hardware.

It is unlawful to reproduce copyright material without the express permission of the copyright holder. Staff and Members must not use the Council’s ICT Systems to access, transmit, retrieve, download, upload, store, distribute or otherwise process any material the copyright for which is or they suspect may be owned by a third party (without the prior authorisation of the copyright holder).

It is the responsibility of Service Managers to identify any data that is of a particularly sensitive nature (and where it is stored). They must also determine whether any specific security precautions are to be taken over and above what is specified in this document and notify these in writing to the IT Manager and GDPR officer.

5.2 Procurement

Before any ICT hardware is procured, or commitment is made to procure, formal approval will be required from the appropriate capital or revenue budget holder. Once the approval has been received a formal request via the ICT service desk should be made outlining the requirement and providing the budget code against which the purchase will be charged.

All purchases of incidental software must be carried out by Breckland ICT (unless a written permission from Breckland ICT to do otherwise is issued), via a service desk request stating the software required and the budget code to be used for recharge. You are forbidden to purchase software / hardware from third-party suppliers without prior written agreement and authorisation from Breckland ICT.

5.3 Inventory

Breckland ICT maintains a computer-based ICT Inventory register. This register includes all major items of ICT hardware, such as application and file servers, PC/laptop/tablet equipment and telephony equipment, but will exclude minor equipment such as telephone handsets and connection cables. A separate register will include all software applications owned or licensed by the Council.

5.4 Physical security

Only authorised persons are allowed access to the secure computer rooms. Emergency access for Health and Safety purposes can be gained by contacting the Property team.

The disclosure of door access codes, or supply of security swipe cards, to unauthorised personnel is not allowed (unless in emergency situations or authorised by Breckland ICT)

Keys for secured areas, equipment cabinets and cupboards must not be handed to unauthorised staff (unless authorised by Breckland ICT).

5.5 Acceptable use of assets

Acceptable use is agreement to adhere to certain standards of behaviour with respect to the proper usage of the Council's ICT assets.

Assets relates to any data, device, software, or other assets of the environment that supports information-related activities, including:

- Hardware: computers, mobile devices, printers

- Software: operating systems, applications (including Web-based apps), utilities, firmware and programming languages

- Services: internet, cloud services, email accounts and other hosted services

- Information and Data: structured data in relational databases, flat files and NoSQL data; unstructured data such as text documents, spreadsheets, images, video and audio files; records in any format

- Networks: wired and wireless networks; telecommunications systems; voice over IP services

5.5.1 Computer equipment

5.5.1.1 Safe custody

Service Managers are responsible for the safe custody and use of the computer equipment within their service areas and should be aware of the location of all portable equipment within their service at all times and in the event of an audit. Such responsibility may be discharged through delegated officers.

Laptops are unfortunately easily stolen due to the nature of their portability. When not in use they should be stored in secure locations and not be on display. This also applies to any other portable equipment such as tablet devices and mobile phones.

ICT equipment must not be left unattended and in full view in a vehicle. If equipment is left unattended in a car for any reason, you should store this equipment in the boot of the car for safekeeping.

5.5.1.2 PCs / Laptops / Tablet devices

You must not in any way change the existing configuration of the Council's software on desktop, laptop, mobile phone or tablet devices.

Trial or evaluation software must not be installed on Council PCs, laptops, tablets or phones without the consent of the Breckland ICT team who will undertake the loading of all software onto devices including any non-standard software.

Files (documents, spreadsheets etc) saved locally to the device (for example on a laptop C: drive) are not backed up by Breckland ICT. If such drives are damaged or otherwise unusable the data on it cannot be recovered. For this reason, Council data should not be held on local drives of any kind.

Devices should not be left unattended whilst logged onto the network. For security reasons always lock your device when left unattended (Windows key & L).

The use of removable media is restricted at Breckland Council. USB ports are locked down on all Breckland Council domain devices. The ability to charge devices by the USB port (such as mobile phones) is permitted.

5.5.1.3 Printers

Breckland ICT will provide access to printers at Breckland offices. General guidance on how to use printers effectively can be obtained from the Breckland ICT service.

Breckland ICT are unable to support any third-party printers that are not situated within Breckland offices.

Printing should always be undertaken using the most cost-effective means available where possible, whether this is through in-house printers or outsourced printing services.

Any paper-based information that may be sensitive should always be disposed of in the blue security bins located within Elizabeth House.

5.5.1.4 Internet

Internet usage may be monitored by Breckland ICT: unauthorised use is a major breach of this policy.

You are expressly forbidden from downloading any software or other executable programs without permission from Breckland ICT. If you identify a need to download software from the internet for evaluation purposes, you must first contact the ICT Helpdesk. Software must not be downloaded in advance of these discussions since the act of downloading may make the Council liable to purchase the software on the supplier's terms and conditions of contract.

You should neither download nor transmit any material that is pornographic, racist, sexist, of an extreme political nature, or which incites violence, hatred or any illegal activity or otherwise may bring the Council into disrepute or information, which could be regarded as sensitive.

5.5.2 Email

All external e-mails and files exchanged over the internet will pass through the

Council's firewall and cloud-based security systems to assist in the prevention of spreading viruses, malicious software or cyber security breaches. However, this is not a complete answer to the problem and any suspicious email or attachments should not be opened. You must report any suspicious emails or attachments to Breckland ICT service desk (helpmeit@breckland.gov.uk or 01362 656277)

Email is not totally secure and no personal, confidential or sensitive material should be sent by email or attached to any email, without careful editing and consideration.

All emails to external sources will include a disclaimer, set by the council.

There is an etiquette associated with composing and sending emails, with the main features:

- Never assume that a message you have sent has been read
- Make arrangements for your email to be forwarded to, or accessed by, someone in your absence (have written permission from the mailbox owner and service manager / director in advance). Consider the use of an automated reply message to warn the sender
- Never send abusive or defamatory messages
- Use an email 'signature' in accordance with the Council standard
- Never send or forward chain letters or other 'unsolicited' mail (SPAM) such as 'virus or other warnings' or advertising
- Resist the temptation to copy any message to more people than is necessary
- Never send any message that might discredit or embarrass the Council

5.5.2.1 Phishing Protection

- Never click any links or attachments in suspicious emails
- If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it
- Report (**do not forward**) the message to the IT Service Desk (helpmeit@breckland.gov.uk or 01362 656277)

- Delete the message

5.5.3 Information and data

Ensure to use information assets in ways that do not put at risk the availability, reliability, or integrity of data, services or resources.

Maintain an awareness of the nature, classification, and handling rules associated with any data that you use in carrying out your duties. In particular, you should consider the following questions:

- Is it confidential?
- Is it personal data?
- Is it sensitive personal data?
- Who needs access to it?
- What retention criteria applies to it?
- What would be the impact if it was lost?
- What would be the impact if it were accessed by people who have no authority or legitimate purpose?

Do not share or discuss confidential information with anyone who does not have a legitimate reason to access that information. Know who you are dealing with when sharing information. Only share information with known individuals (or previously unknown individuals who have validated their credentials) who have a legitimate reason to access the information.

5.5.4 Instant Messaging Service (IM)

Instant Messaging services provide real-time communication between two or more people based on typed text. The text is conveyed via devices connected over the Internet or an internal network/intranet.

Instant Messaging services presents certain risks, including non-compliance with data protection laws such as issues around consent, data transfer, access, deletion and portability.

Instant Messaging should not be used as a substitute for email and should be used only for questions or announcements that are short and need to be communicated immediately.

Private use of instant messaging for 'recreational' chatting on Council devices is not permitted.

5.6 Remote and home working

Some staff and Members use the Council's ICT services at home or at a remote location: all aspects of this policy still apply.

The Council provides a single method of remote connection to office-based ICT services and restricts those parts of the network and software applications that are available to home/remote workers.

The council employs a virtual private network (VPN) solution to provide secure remote working for council officers to enforce data protection for Councils data and services when accessed from remote locations.

As part of the Council's obligations regarding PSN all users working remotely must use Breckland Council supplied ICT equipment when undertaking Breckland Council work. This includes both staff and members and applies to any activity that makes use of council systems (including but not limited to emails and the use of applications).

The only exception to this is the use of mobile phones for calling, where personal devices are permitted where appropriate.

External access to the Council's ICT infrastructure and systems by suppliers, 3rd parties and external temporary staff is not permitted without prior written authorisation from Breckland ICT.

5.6.1 Employee & Member responsibilities

- Ensure the physical security of a home office or remote working environment
    - Is there enough room to house the required equipment safely?
    - Is it in a separate area of the living accommodation?
    - Can the work area be secured when not in use?
    - Who else has access to the work area?
    - Will the equipment be visible from outside?
    - What is the likelihood of theft in the surrounding area?

    - Can paper documents be locked away securely?
    - Is there adequate and reliable power supply to the work area?

- Ensure that the environment is conducive to home or remote working (e.g., a dedicated quiet room free from family interruptions)
- Prevent Council devices, such as laptops, mobiles and other forms of hardware, from being accessed by other household members
- Ensure data is saved centrally through the Council's infrastructure, and never on the local machine
- Ensure the security of confidential information relating to the Council and customers
- Operate a clear desk policy and be aware of leaving any Council or personal information in view of monitors, as this information may be seen during video conference calls
- Ensure WIFI security - Create a strong, unique password, rather than relying on the automatic password the router came with, and enable WPA2 network encryption
- Ensure regular connection to the Council infrastructure for updates to virus protection
- Take reasonable care of their own health and safety and that of anyone else who might be affected by what they do including other family members, neighbours and visitors
- Undertake a health and safety risk assessment on their home workstation. This is a self-assessment and the details can be found at: https://www.hse.gov.uk/home-working/index.htm

5.7 Mobile devices and portable media

Breckland Council provided mobile devices are the property of Breckland Council and should be used for legitimate business purposes only.

Users must not use, try to use, or let anyone else use staff/member mobile communications devices for:

- Deliberately viewing, copying, creating, downloading, saving, printing or distributing any material that:

    - Is sexually explicit or obscene
    - Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
    - Contains material the possession of which would constitute a criminal offence
    - Promotes any form of criminal activity
    - Contains unwelcome propositions
    - Involves gambling, multi-player games or soliciting for personal gain or profit
    - Contains images, cartoons or jokes that may cause offence
    - Brings Breckland Council into disrepute or exposes the Council to legal action
- Making offensive, threatening or harassing calls
- Use in contravention of Regulation 104 of the Road Vehicles (Construction & Use) Regulations, 1986; i.e. using a mobile device whilst driving

Where a user has been provided with a council mobile device the following also applies:

- No hardware, software or related components should be added to the mobile device without the approval of Breckland ICT
- Mobile devices should only be allowed access to the Council network at the discretion of the ICT Manager who will approve the connection type as secure, protected and supported
- No personally owned equipment may be attached to the Council network
- All mobile devices and associated memory cards must be encrypted or password protected wherever technology allows
- Mobile devices should not be used to record conversations or images without the knowledge or consent of the individuals concerned

Users have a responsibility to utilise the Breckland Council's communications resources and services in a manner that is consistent with the Breckland Council's standards of business conduct.

Mobile communications devices should be securely stored when not in use. Handset covers provide a degree of physical protection. Users may be liable for repair or replacement costs, should their handset be damaged or lost.

Any such damage or loss should be reported to the Breckland ICT service desk (helpmeit@breckland.gov.uk or 01362 656277) you may also be required to contact the Police for an incident number in the event of loss or theft.

5.8 Access control and passwords

This policy will grant users, information, network, Operating System and application access based on the principle of least privilege, which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task.

5.8.1 User "permissions"

Access to the Breckland Council network and the ICT services available on ICT is controlled by Breckland ICT: users are given network "permissions" according to their job requirements.

A Service Manager can request extensions to such permissions (e.g. which network folders the user is allowed to access, or which features of Microsoft Outlook are available).

Each major software application will have a similar policy regarding user access permissions which is defined by the system "owner" in association with Breckland ICT.

5.8.2 Allocation of user IDs and passwords

Domain passwords are allocated by Breckland ICT (NB application passwords are issued by business system owners).

The initial allocation of passwords, and any resetting of forgotten passwords, will be formally authorised by the service owner of the software or in the case of domain password by Breckland ICT.
Service owners are responsible for reviewing users of their systems at regular intervals and for removing users who have left.

The Council's HR service will be responsible for notifying Breckland ICT of staff starters and leavers or where staff change job function so that their access rights can be modified. Democratic services will be responsible for notifying Breckland ICT of member starters of leavers. The process is initiated via the ICT pages on the Breckland Intranet.

Authorisation is required at Service Manager/Line Manager level for system access.

Users needing access to emails accounts / file locations of staff who are unable to work due to sickness or absence can only be granted if there is written authorisation from the relevant assistant director or HR Manager.

If access is required to member email accounts/file locations, this will only be done with authorisation from the Chief Executive.

5.8.3 Review of User Access Rights

User access rights and privileges will be reviewed by System Owners and Service Manager/Line managers following promotion; demotion; a change in role; on commencement of a project; on closure of a project; and, on termination of employment.

5.8.4 Use of passwords

- All passwords must be a minimum of sixteen characters, both alpha and numeric, include at least one special character and have a mix of upper and lower case.

- Passwords must not be disclosed or shared with anyone else, and there should never be a record of a password in a manner that is insecure (e.g. written down on paper)

- Lost or forgotten passwords will be reported to the ICT service desk (helpmeit@breckland.gov.uk or 01362 656277)

- Passwords used on Breckland Council systems should not be also used for private email and social media sites (for further guidance on password security contact the Breckland ICT service)

5.9 Personally owned devices

Breckland Council prohibits the use of personal devices to process council data, or access council systems and infrastructure. This is to ensure the integrity of Breckland Council's IT security and to meet PSN requirements.

5.10 Exchanging data with external organisations

The physical or electronic exchange of any software and/or data between the Council and external bodies should be subject to formal agreement which include the identification of data formats, carrier arrangements and documented verification of receipt.

Appropriate standards will be applied to the electronic exchange of data between the Council and external agencies. Wherever practicable, software applications that depend upon Electronic Data Interchange (EDI) facilities should include precautions to deal with the possibility that data has been intercepted or modified during transmission, along with checks that data has been dispatched and delivered correctly. Data that has been identified as being of a specifically sensitive nature will not be transmitted unencrypted across unsecured EDI links. Such data may be transmitted unencrypted across secure EDI links or other secure networks such as the Government Secure Intranet. All security controls applied to EDI links will be agreed with the relevant trading partners and compatibility with industry standards will be sought wherever possible.

When communicating any data that might be classed as personal or sensitive the GDPR officer should be consulted (prior to information being issued) to ensure there is no breach of the GDPR or Data Protection Act.

5.11 Disposal of information and ICT equipment

All waste paper must be disposed of with due regard to its sensitivity. Confidential output must be stored in the blue wheelie bins provided for this purpose. Less sensitive waste paper can be disposed of in the recycling bins.

Magnetic media, such as CDs, USB devices and hard drives etc. must be disposed of by informing the Breckland ICT service desk (helpmeit@breckland.gov.uk or 01362 656277), who will arrange for a suitable means of disposal.

5.11.1 Disposal of PCs and other ICT equipment

The Waste Electrical and Electronic Equipment (WEEE) Directive came into force in January 2007 and aims to both reduce the amount of WEEE being produced and encourage everyone to reuse, recycle and recover it.

The following procedure should be followed throughout the disposal cycle of all end-of-life PCs and laptops.

All redundant ICT equipment will be disposed of by arrangement with the Breckland ICT Service. Before disposal, the equipment concerned must be written off in accordance with Financial Regulations and removed from the Council's general asset register and also from Breckland ICT inventory of ICT equipment. All asset, equipment and software licensing labels should be removed prior to disposal.

In the case of attached disks or other storage devices, specific care will be taken to ensure that all systems software and data are erased from disk prior to disposal of the assets (or by prior arrangement the 3rd party is certified to erase Breckland Council data off premises). Any third party retained by the Council for disposal of equipment will be contractually required to ensure that data on faulty disks is destroyed.

Under no circumstances should redundant PC equipment be disposed of by depositing items in the Council's bins or skips.

Elements of PC systems, printers and individual components may be disposed of as General Non-Hazardous Waste i.e. keyboard or mouse.

5.12 Operational management

5.12.1 Documentation

All Council ICT operating procedures and system processes outlined in the Information Security Policy must be documented. Operating procedures must be documented to an appropriate level of detail for individuals/departments using them and should include the following areas:

- Processing and handling of Information (information classification, confidentiality requirements)
- Work scheduling requirements (considering interdependencies, completion times etc)
- Instructions and guidance for handling errors
- Contact and report details in the event of unexpected operational issues
- Procedures for handling special outputs (e.g. payslips)

- System restart and recovery procedures in the event of system failure
- Procedures for all 'housekeeping' functions
- Procedures for audit and assurance reviews

5.12.2 Change management

Changes to the Council ICT infrastructure must only be undertaken by authorised personnel working in an ICT function/capacity (or contractors, vendors etc., authorised by Breckland Council ICT) and are subject to auditable change management procedures.

Changes to the Council ICT infrastructure and operational systems must be controlled with a formal, documented change control procedure. The change control procedure should include references to:

- A description and reason for the change
- Information about any testing phase(s)
- Impact assessment including security, operational etc
- Formal approval process – managerial approval and authorisation prior to proceeding with changes which may have a significant impact
- Communication to all relevant people of the changes which includes:
    - Advance communication/warning of changes
    - Proposed schedules
    - Description of reasonably anticipated outcomes provided to all relevant personnel
    - Procedures for aborting and rolling back if problems occur
    - Processes for planning and testing of changes, including fallback (abort/recovery) measures
    - Documentation of changes made and all the steps taken in the change management process
    - Identification of significant changes and relevant risk assessments - including analysis of any potential impact and necessary countermeasures or mitigation controls

All changes to the ICT infrastructure need to be assessed for impact on the security of data and information as part of standard risk assessments.

5.12.3 Separation of Development, Test and Operational facilities

Development and test environments must be separated from live operational environments in order to reduce the risk of accidental changes, configuration/data incompatibilities and unauthorised access. Development and live environments must be segregated by the most appropriate controls including:

- Running on separate computer/systems
- Running on different domains
- Use of test/temporary usernames and passwords

Where practical, separation of duties should be maintained to ensure no one individual can gain unacceptably high levels of access to the Council's ICT systems and information processing facilities.

5.12.4 Capacity management

Breckland ICT must monitor the capacity demands of the Council's systems and make projections of future capacity requirements so that adequate power and data storage requirements can be fulfilled.

Utilisation of key ICT system resources must be monitored so that additional capacity can be brought on-line when required.

5.12.5 System acceptance

All departments must inform Breckland ICT, of any new software requirements or of any upgrades, service packs, patches or fixes required. If a requirement involves a significant change or the introduction of a new ICT system, Breckland IT must be consulted as per section 5.2 of this policy.

Appropriate levels of testing must be undertaken for new ICT systems, product upgrades, patches and fixes before the acceptance and release into a live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve appropriate authorisation levels.

Software must be monitored for service packs, updates and patches, which should be tested and applied as soon as possible when released and once it has

been approved. Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment which duplicates the 'live' operational system.

5.12.6 Patching

ICT system servers should have critical security patches applied as soon as they become available. All other patches and updates are applied at part of a monthly software patching process. There must be a full record of which patches have been applied and when.

To enable these patches to be distributed to Breckland Council devices there is a need for the device to be connected to the Breckland Council network on a regular basis. Should you be expecting to work remotely for a continuous period of 10 days or more you are required to log a call with the Breckland Council ICT service desk to discuss alternative methods to ensure software patching is maintained on the device.

5.12.7 Virus protection and controls against malicious code

Anti-malware/Anti-virus software must be installed and maintained on all workstations and servers and any other computing device which uses software to function and is capable of being scanned by Anti-malware/Anti-virus software.

The software must be from an established vendor with consistent results in recognising and removing all types of malware. All updates must be installed as soon as they are available. A regular review of all business-critical systems must be conducted to identify all software running on the systems. Any unauthorised files or software must be formally investigated and deleted as appropriate.

To protect systems from malware, users must not:

- Install software from any external source, including the internet, CD, USB memory sticks, etc, on their workstation.
- Add their own screensavers, desktop images, photos or utilities to the workstation.

All software must be approved and installed by Breckland ICT. Software must also be controlled to ensure compliance with licensing and other legal requirements.

Malware and viruses can be introduced through e-mails and users must be vigilant and follow ICT guidelines on dealing with suspicious e-mails and

attachments. If there is uncertainty with the safety of particular e-mails or attachments, Breckland ICT should be contacted.

Breckland ICT must ensure that all e-mail and attachments are checked for malware and viruses at the point of entry into the network.

All Breckland Council laptop and desktop devices must utilise software firewalls to provide a layer of protection against cyber security breaches. These software firewalls should be enabled at all times unless disabled by Breckland Council ICT for a specific reason.

5.12.8 Backups

Breckland ICT must ensure that regular backups of Information, data and ICT systems configuration are routinely carried out, and copies of those backups are stored in a secure, off-site location, to ensure recovery from unforeseen events, system failure, accidental or deliberate loss of information or facilities - in line with Disaster Recovery Procedures.

Data held on the local drives of a PC or laptop is not backed up.

All 3rd party/software vendors hosting or supplying services/facilities containing or handling Council information and data must ensure appropriate, secure backup routines and facilitate access for the Council's internal audit requirements when necessary.

Critical paper files must be identified and backed up with either a scanned digital copy or complete photocopies and stored on the Council's ICT infrastructure and systems.

Following the departure/resignation of an employee or member, Breckland ICT will deactivate the account following confirmation of change from HR and ensure that emails and files related to the employee's or member's role be stored or archived for a period of at least 1 month before being deleted. This is important to ensure that an audit trail is maintained of any important issue regarding the work the employee or member was responsible for prior to leaving the Council.

For all critical and corporate file and applications servers, sufficient back-ups will be held at remote sites to enable the recovery of data should a disaster at any one Council site result in the complete permanent loss of ICT facilities at that site.

5.12.9 System disposal

After a system has been designated to be removed from service, Breckland ICT must perform an audit of the system components and remaining data. Objectives include the following:

- Information Preservation – Identifying data that must be archived for long-term storage based on classification, and document retention requirements
- Media Sanitisation – After standing data has been removed, the system must be decommissioned with the intention of shutdown. Media sanitisation reasonably guarantees sensitive information cannot be easily reconstructed or retrieved
- Hardware and Software Disposal – Following procedures covered earlier in this policy document, there must be assurance that every disposal is properly managed

5.12.10 Security of system documentation

All Council ICT system documentation must be protected from unauthorised access. This includes documentation that has been created by the Breckland ICT service or any other departmental IT employees (this does not include manuals that have been supplied with software). Examples of the documentation to be protected include descriptions of:

- Applications
- Processes
- Procedures
- Data structures
- Authorisation details

5.12.11 Information transfer policies and procedures

Processes and procedures and must be implemented to protect the transfer of information through all available methods and formats e.g., e-mail, EDI etc. Procedures must be designed to protect exchanged information against:

- Interception
- Copying

- Modification
- Misrouting
- Destruction

Information and data must be protected with appropriate controls based on the information's classification.

Formal agreements for the transfer of Information between the Council and external organisations must be made and reviewed on a regular basis.

5.12.12 Event logging

Council ICT system audit logs must be kept for a minimum of six months which record exceptions and other security related events. As a minimum, audit logs must contain the following information:

- System identity (Workstation name)
- User ID (employee number)
- Successful/Unsuccessful login
- Successful/Unsuccessful logoff
- Unauthorised application access
- Changes to system configurations
- Use of privileged accounts (e.g. account management, policy changes, device configuration)

Access to the logs must be protected from unauthorised access that could result in recorded information being altered or deleted. System administrators must be prevented from erasing or deactivating logs of their own activity. Access to logs should be provided for the Council's internal audit requirements when necessary.

5.12.13 Network security management

The management and security of the data and communications network is critical to ensuring the integrity and security of the Council's systems and data. The following controls must be applied:

- Operational responsibility for networks should, wherever possible, be separated from computer operations activities

- There must be clear responsibilities and procedures for the management of remote equipment and users

- Where appropriate, controls must be put in place to protect data passing over the network e.g. encryption

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Encryption must be used on the network to protect information and data and to prevent information being intercepted.

5.12.14 Encryption

Encryption must be used to provide confidentiality of data that may or will be accessed by an untrusted entity. The following controls must be applied:

- Encryption in transit should be implemented for all data flows. Data may be transferred in clear where the data flow is entirely within a single trusted network segment

- Encryption at rest should be used for all storage components that hold non-public data

5.12.15 Cloud computing

Agreements with suppliers should include requirements to align to the Council's information security policy and risks. Supplier agreements must include:

- A process for suppliers to propagate the Council's security requirements throughout the supply chain if suppliers subcontract for parts of ICT service provided to the Council

- A monitoring process and acceptable methods for validating that delivered ICT products and services are adhering to stated security requirements

- Assurance that critical components and their origin can be traced throughout the supply chain

- Assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features

- Definition of rules for sharing of information regarding the supply chain and any potential issues and compromises among the Council and suppliers

- Specific processes for managing ICT component lifecycle and availability

and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements

5.13 Privacy and protection of personally identifiable information

Personal data is information that relates to an identified or identifiable individual.

Obligations under the UK GDPR will vary depending on whether the organisation holding personal data is a controller, joint controller or processor.

Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.

If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

Processors act on behalf of, and only on the instructions of, the relevant controller.

Controllers shoulder the highest level of compliance responsibility – and must comply with, and demonstrate compliance with, all the data protection principles as well as the other UK GDPR requirements. Controllers are also responsible for the compliance of their processor(s).

The Information Commissioner's Office (ICO) and individuals may take action against a controller regarding a breach of its obligations.

The primary principles include:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)

- Accountability

The Council's obligations in regard to security of personal information:

- Personal information must be stored and processed securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

- Protection of personal information must consider risk analysis, organisational policies, and physical and technical measures, as are covered in this policy.

- Measures must ensure the 'confidentiality, integrity and availability' of systems and services and the personal data processed within them.

- Measures must also enable the restore of access and availability to personal data in a timely manner in the event of a physical or technical incident

- Any proposed system changes that could potentially impact personal data, must undertake a Data Protection Impact Analysis (DPIA)

- There must be appropriate processes in place to test the effectiveness of these measures and undertake any required improvements.

If the Council is affected by an incident which involves (or is likely to involve) a breach of personal data, then there is an obligation under the GDPR to notify the ICO.

6. Special arrangements for Members

As well as being bound by all of the conditions of this policy, Members are also subject to the following additional conditions:

- Where a member is found to be in breach of this policy any subsequent enforcement actions will be in accordance with Constitution and the Code of Conduct for Members.

- Members are provided with ICT services by the Council to assist them with the fulfilment of their duties as an elected member. Use of Council-provided ICT services for commercial or party-political activities is not permitted.

7. Cybersecurity

As with most local authorities, the council relies heavily on access to the internet. There are several ICT systems that have an internet presence and there are several different access mechanisms to information (Wi-Fi, physical networking, smartphones, tablets). All of these access mechanisms present potential threats to cyber security. The Council therefore deploys a layered range of tools and good ICT practices to minimise the risk to its information and systems.

The Council implements security controls and good practice to enable it to achieve compliance with Public Services Network (PSN) standards. This requires the Council to ensure that systems are security patched and that the Council has regular penetration tests of its network/systems that are performed by a third party.

The Council deploys a range of technology and processes to help it achieve and maintain a solid security platform. These range from up-to-date firewalls and core networking equipment, through cloud-based antivirus controls and secure wireless connectivity to encrypted devices, two factor authentication and mobile device management.

The Council subscribes to the Cyber-security Information Sharing Partnership (CiSP) and is an active member of the East of England WARP (Warning, Advice & Reporting Point) which supports the sharing of up-to-date advice on any ongoing security threats or actual incidents. In addition, the Council liaises closely around cybersecurity with neighbouring local government organisations such as Norfolk County Council and a number of district councils.

8. Exceptions

Any exception to the policy must be approved and recorded by the ICT & Digital Manager in advance, and if appropriate, reported to CMT.

9. Appendix 1 - Glossary

Application	A set of specialised programs and associated documentation to carry out a particular application such as Council Tax or Planning
Backup	To save data, applications and systems. ICT usually consists of writing everything contained on a system or PC to another form of electronic media, such as a¼ inch tape cartridge or another hard disc. This is then available if any information is lost or corrupted.
Computer System	Is a central processor together with its associated peripheral equipment.
Cyber Security	the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this
Data	Information or data that is stored on a computer. ICT can be anything from a word-processing document to a number.
DPO (Data Protection Officer)	The designated role within an organisation that is responsible for overseeing data protection strategy, implementation, and ensuring compliance with data protection laws and regulations.
Email	Electronic Mailing System for both internal and external systems.
ECHR	European Convention on Human Rights
Hardware	The physical components of a computer system, including peripherals (e.g. processor, keyboards, screens, printers).
ICT	**I**nformation and **C**ommunication **T**echnology.
IS/IT	**I**nformation **S**ystems/**I**nformation **T**echnology.
LAN	A LAN is a network of computers and other devices in a specific geographical area that are linked together to share resources and data.
Laptop	Portable Personal Computer.
Login name	This is the name you type when prompted. To log in to a certain system e.g. Council Tax, etc. This will normally be followed by a password
Firewall	Protect a computer network or system from unauthorised access
Network password	Password used to give authorisation to access certain computer systems.
P.C.	Personal Computer
PSN	Public Sector Network – Secure data network linking Government bodies

Security Systems	System that is in place to protect ICT from unauthorised use that adheres to the Reference Data Protection Act and Computer Misuse Act.
Software	Consists of programs, routines, procedures and their associated documentation, which can be implemented on a computer system.
Systems	Usually refer to individual applications e.g. Council Tax Benefits, Environmental Health, logged onto from the main log in. Can also refer to the computer operating system e.g. Windows, DOS or UNIX
USB	universal serial bus, a standardized technology for attaching peripheral devices to a computer.
Virus	A program hidden among legitimate software and loaded onto an unsuspecting users computer. When triggered i.e. running that program, the virus may cause damage to data on that computer.
WAN	A WAN is a network that connects devices over a large geographic area, like cities or countries, often using public infrastructures such as telephone lines or satellites.
WPA-2 (Wi-Fi Protected Access II)	WPA2 is a more secure version of the original WPA, a security tool used to keep Wi-Fi networks safe. Introduced in 2004, it helps protect your data online by using advanced methods of encryption, mostly Advanced Encryption Standard (AES).